UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

STRIKE 3 HOLDINGS, LLC, Plaintiff, vs. JOHN DOE subscriber assigned IP address 74.73.129.18, Defendant.	:	Case No. 1:24-cv-02326-DEH

DECLARATION OF PATRICK PAIGE IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO TAKE DISCOVERY PRIOR TO A RULE 26(f) CONFERENCE

[Remainder of page intentionally left blank]

DECLARATION OF PATRICK PAIGE IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO TAKE DISCOVERY PRIOR TO A RULE 26(f) CONFERENCE

I, Patrick Paige, do hereby state and declare as follows:

1. My name is Patrick Paige. I am over the age of 18 and I am otherwise competent to make this declaration.

2. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.

3. I am a Managing Member at Computer Forensics, LLC a Florida based expert computer forensics company.

4. For approximately 20 years, I have worked in the computer forensics industry.

5. During this time, I have conducted forensic computer examinations for:

   a. Broward County Sheriff's Office (BSO);

   b. Federal Bureau of Investigation (FBI);

   c. U.S. Customs and Border Protection (CBP);

   d. Florida Department of Law Enforcement (FDLE);

   e. U.S. Secret Service;

   f. Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); and

   g. Various municipalities in the jurisdiction of Palm Beach County.

6. I have taught over 375 hours of courses in computer forensics ranging from beginner to advanced levels.

7. I have had students in my courses from various government branches, including: (a) sheriff's offices; (b) agents from the Federal Bureau of Investigation; (c) agents from the Bureau of Alcohol, Tobacco, Firearms and Explosives; (d) agents from the Central Intelligence Agency, and (e) individuals from other branches of government and the private sector.

8. I have been called to testify as a fact and expert witness on numerous occasions in the field of computer forensics in both trial-level and appellate proceedings before state, federal, and military courts in California, Florida, Indiana, New Jersey, New York, and Pennsylvania.

9. No court has ever refused to accept my testimony on the basis that I was not an expert in computer forensics.

10. I have worked with a program called Wireshark since 2004.[1] I first began using this software at the Palm Beach County Sheriff's Office within the Computer Crimes Unit. In that role, I used Wireshark to conduct online investigations where individuals transmitted contraband images to me during online chat sessions. In private practice, I have also used Wireshark to monitor network traffic while investigating network intrusion cases. Later in my career I also used this software to examine PCAPs associated with BitTorrent transactions.

11. In 2019, I obtained my certification as a Wireshark Certified Network Analyst.

12. I was retained by Strike 3 Holdings, LLC ("Strike 3") to individually analyze and retain forensic evidence captured by its infringement detection system.

13. In this case, Plaintiff claims that its infringement detection system, VXN Scan, recorded numerous BitTorrent computer transactions between the system and IP address 74.73.129.18 in the form of PCAPs.

14. PCAP stands for "Packet Capture." A PCAP is a computer file containing captured or recorded data transmitted between network devices. In short, it is a recording of network traffic.

[1] Initially, Wireshark was named "Ethereal" when it was released in 1998. However, it was renamed "Wireshark" in 2006.

15. Here, the PCAPs would evidence particular IP addresses connecting to VXN Scan and sending pieces of a computer file (which allegedly contains a piece of an infringing copy of Plaintiff's works) to VXN Scan. The PCAP contains a record data concerning that transaction, including, but not limited to, the Internet Protocol (IP) Addresses used in the network transaction, the date and time of the network transaction, the port number used to accomplish each network transaction, and the Info Hash value that the VXN Scan used as the subject of its request for data.

16. For this case, I received a PCAP from Strike 3 containing information relating to a transaction initiated on 03/11/2024 15:21:45 UTC involving IP address 74.73.129.18.

17. I used Wireshark to view the contents of this PCAP.

18. In reviewing the PCAP, I was able to confirm that the PCAP is evidence of a recorded transaction with IP address 74.73.129.18 initiated at 03/11/2024 15:21:45 UTC. More specifically, the PCAP evidence shows that within that transaction, IP address 74.73.129.18 uploaded a piece or pieces of a file corresponding to hash value 04D1E15B09618A4312212EDD4AA7534ABB8DCF96 to VXN Scan.

19. To be clear, the hash value 04D1E15B09618A4312212EDD4AA7534ABB8DCF96 recorded in the PCAP is the "Info Hash." The "Info Hash" is *not* the hash value of the movie file itself.

20. A hash value is an alpha-numeric value of a fixed length that uniquely identifies data. Hash values are not arbitrarily assigned to data merely for identification purposes, but rather are the product of a cryptographic algorithm applied to the data itself. As such, while two identical sets of data will produce the same cryptographic hash value, any change to the

underlying data – no matter how small – will change the cryptographic hash value that correlates to it.

21. The entire file being shared has a hash value (*i.e.*, the "File Hash"). Files are shared on BitTorrent by breaking them down into smaller pieces. To find and re-assemble these pieces, *i.e.*, to download the file using BitTorrent, a user must obtain a ".torrent" file for the specific file that has been broken down into pieces. Each ".torrent" file contains important metadata with respect to the pieces of the file. When this data is put into the cryptographic algorithm, it results in a hash value called the "Info Hash."

22. The "Info Hash" is the data that the BitTorrent protocol uses to identify and locate the other pieces of the desired file (in this case, the desired file is the respective file for the infringing motion pictures that are the subject of this action) across the BitTorrent network.

23. Using the Info Hash, a user may collect all the pieces of the desired file (either from the user that shared the original piece or from other members of the BitTorrent swarm), to create the playable movie file.

24. Once the user has the playable movie file, the user could: (1) calculate the movie's File Hash value, and (2) visually compare the playable movie file to its copyrighted work to determine whether they are identical, strikingly similar, or substantially similar.

25. *Any* change in the underlying movie file (including converting the file to a different format, changing the resolution, etc.) will result in the algorithm calculating a different File Hash value. As such, unless two files have the exact same File Hash, visual comparison of two files is the best method by which to determine whether one movie file is a visual copy of another.

26. Based on the foregoing, my experience in working with peer-to-peer networks and BitTorrent protocols, and my review of the PCAP related to Work No. 1 in Exhibit A of the Complaint, I can conclude that the PCAP provided to me in this matter is evidence which supports the allegation that IP address 74.73.129.18 engaged in a transaction that included the transmission of a piece or pieces of a file, in response to a request for data relating to Info Hash value 04D1E15B09618A4312212EDD4AA7534ABB8DCF96, in a transaction initiated at 03/11/2024 15:21:45 UTC.

27. I have read David Williamson's declaration which describes the design and operation of VXN Scan which recorded the PCAP I examined. Based on his declaration, I believe the PCAP I reviewed is a true reflection of a transaction that took place and that the PCAPs which Strike 3 stores are unalterable.

28. Based on my experience in similar cases, Defendant's ISP Spectrum is the only entity that can correlate the IP address to its subscriber and identify Defendant as the person assigned the IP address 74.73.129.18 during the time of the alleged infringement. Indeed, a subpoena to an ISP is consistently used by civil plaintiffs and law enforcement to identify a subscriber of an IP address.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 25th day of March 2024.

PATRICK PAIGE

By: _____